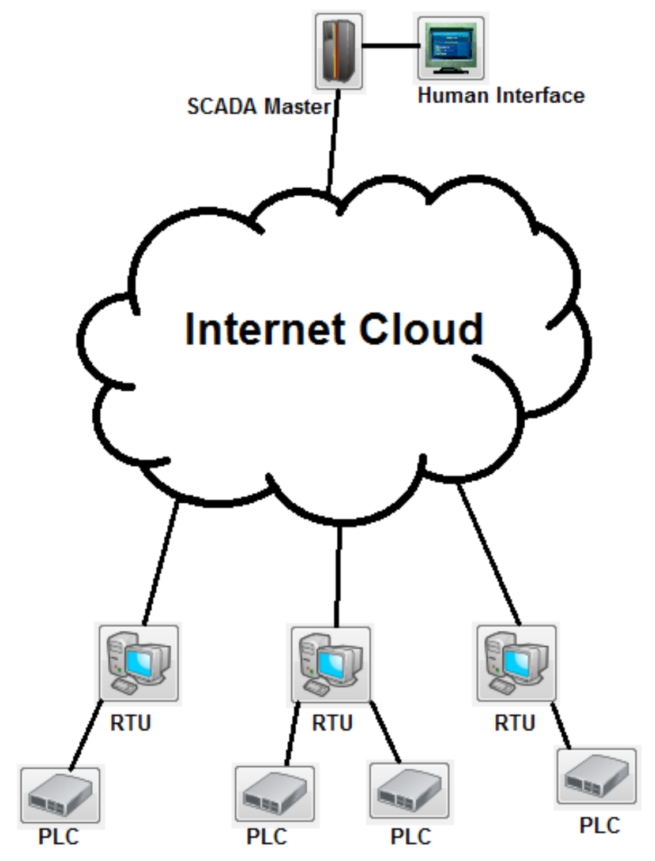
Cross-layer Mischief in Networked Control Systems

ECE 18-637 Project Poster
May 2014, Pittsburgh PA

Greg Nazario, Michael Rosen, Lawrence Jackson and Michael Hankowsky

1. Background

Industry and infrastructure rely more and more on networked control systems to monitor and maintain various plants and remote stations. From water treatment to chemical processes, most of these rely on the SCADA model to control and receive data from the various, often distributed, actuators and sensors. However, the SCADA model, initial implemented on telephone lines, is moving onto the internet and this model was never designed with security in mind. Thus, securing these vital, insecure infrastructure is extremely important. Already, some attacks such as Stuxnet and the Maroochy Shire Council's water treatment plant incident illustrate the need for better security in control system networks. Thus, having a framework to model these complex system is a solid step forward for research in this area.

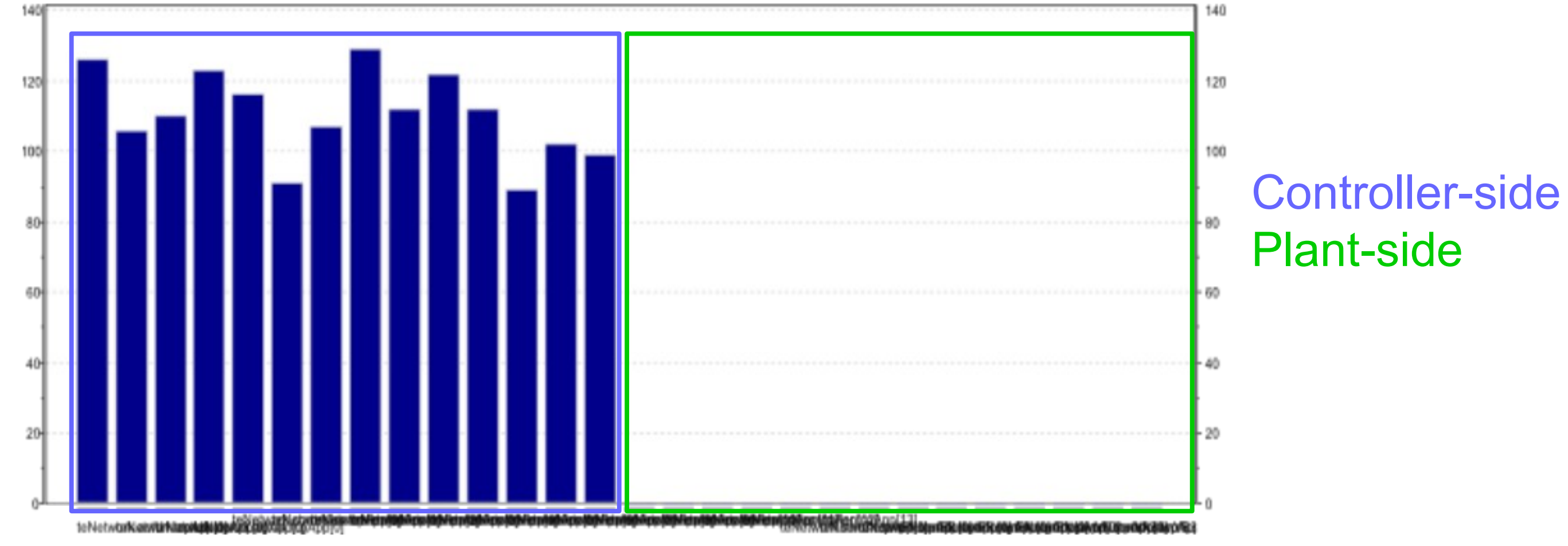


The SCADA system can be broken into a remote side and a local side. The remote side is composed of Remote Terminal Units and Programmable Logic Controllers, these control the actuators and send sensor data to the central SCADA master. This mast issues commands to the RTUs and presents a nice interface to human operators.

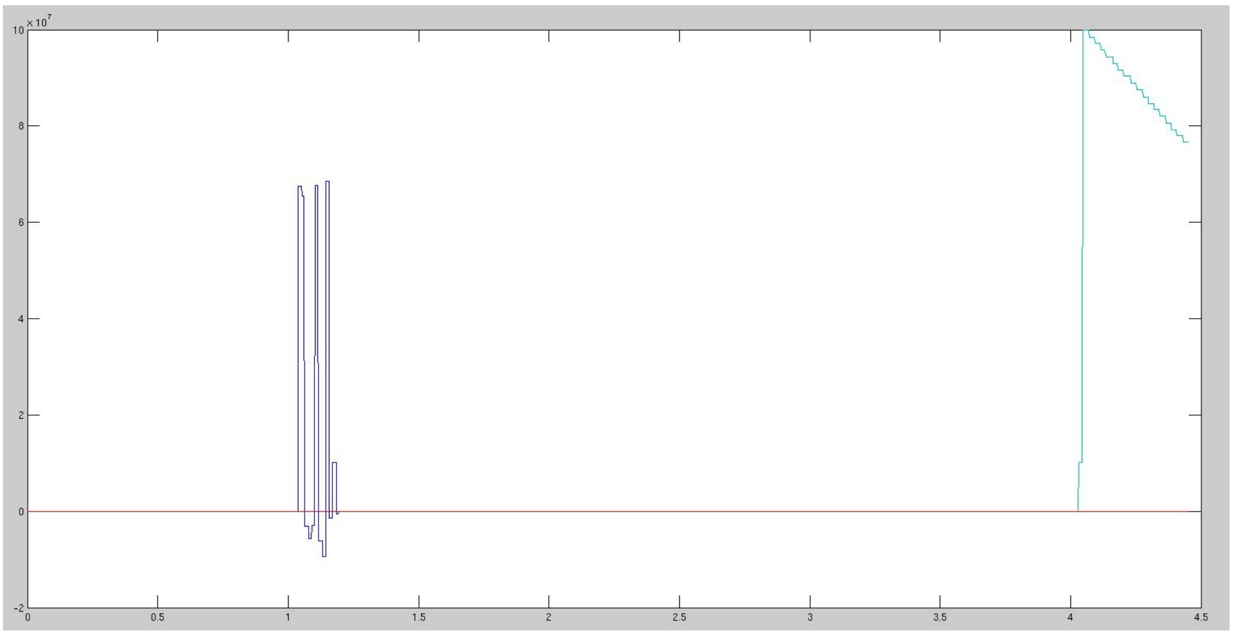
3. Attack Model

Several attacks were considered for disrupting the MATLAB simulation and breaking the equilibrium. One of these was a simple Denial of Service attack, in which the wireless plant-side network would be attacked to prevent communication from the sensor and to the actuators. Another was a spoofing attack in which packets from a sensor where spoofed and the value from the senor appeared to be constant to the controller.

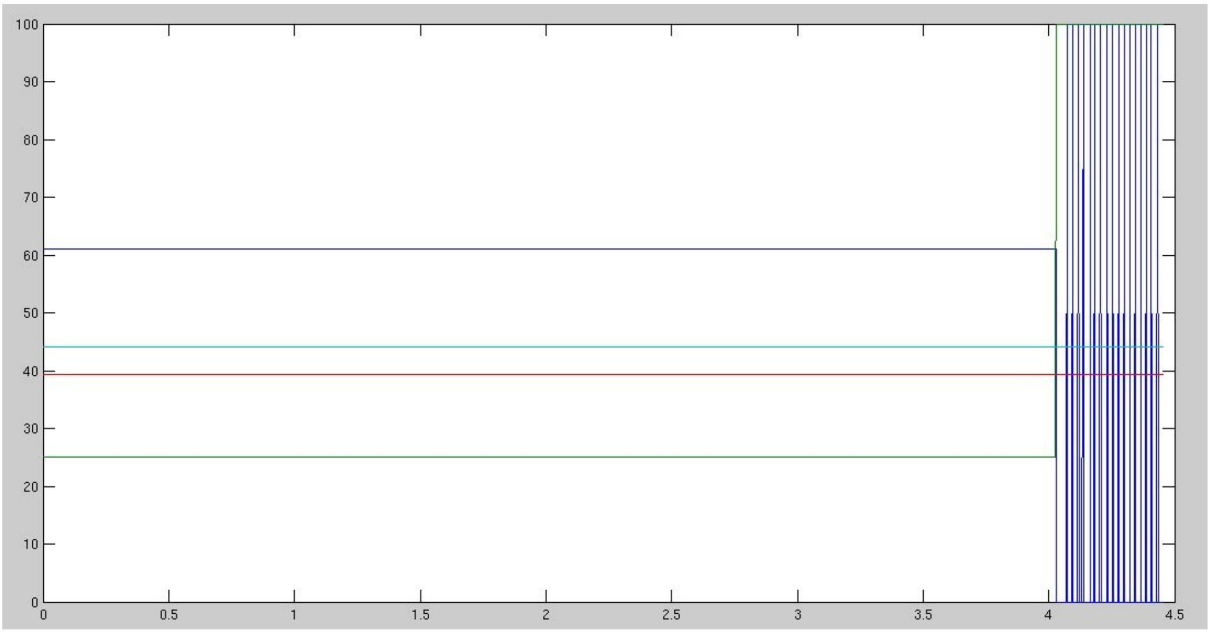
OMNeT++ Network Packets Received during DoS



MATLAB Controller during Spoofing

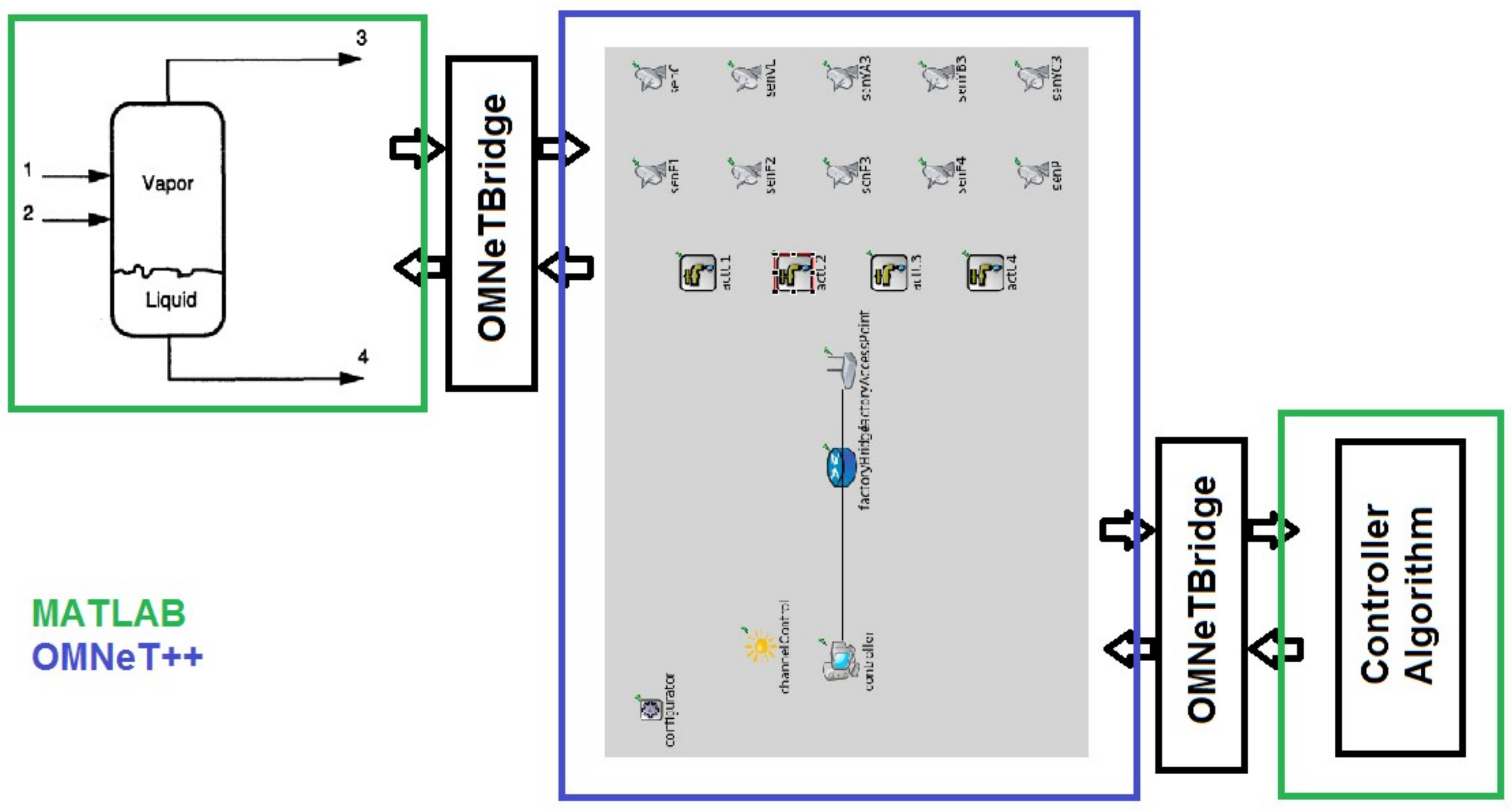


MATLAB TE System during Spoofing



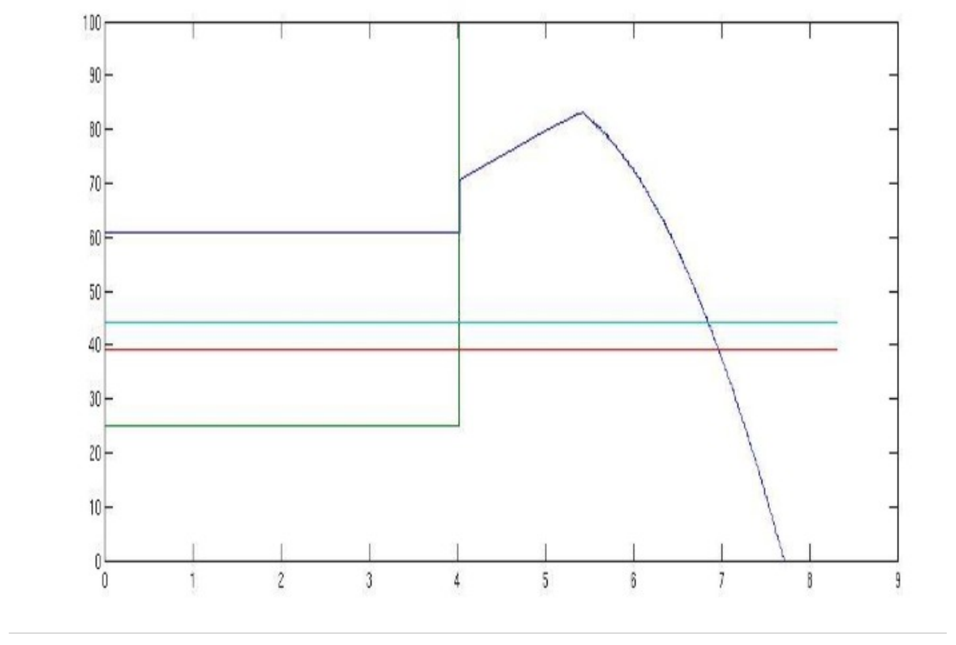
2. Implementation

The simulation framework is broken into three distinct pieces: the OMNeT++ network model, the MATLAB simulation and the OMNeT++ bridge. OMNeT++ is used to simulate the network side of the control system, while MATLAB is used to model a basic Tennessee-Eastman process. The OMNeT++ bridge is used to transfer data from the MATLAB model to the OMNeT++ simulation and back.

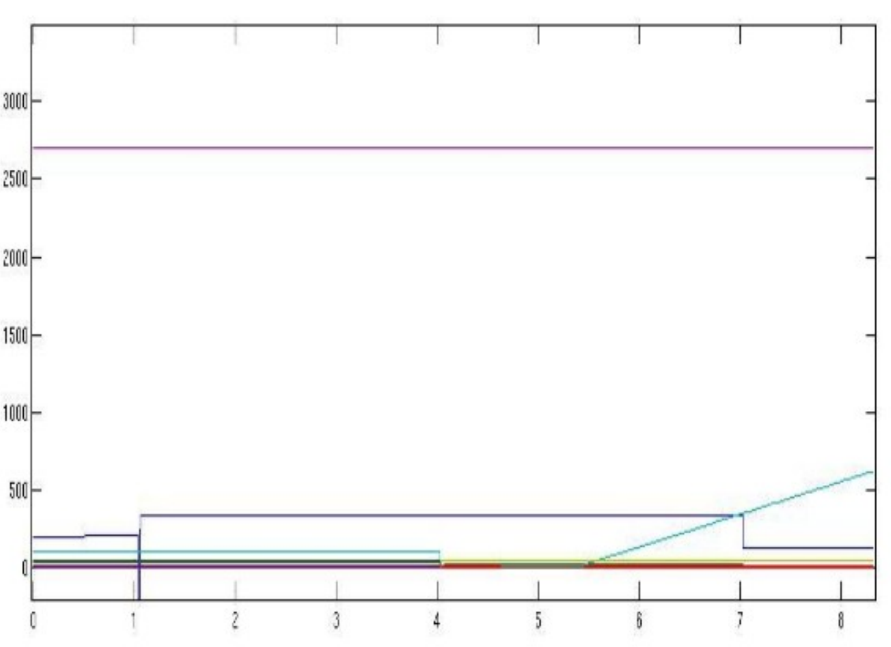


The Tennessee-East process is a basic chemical process. For our purposes, it served as a simple MATLAB model to plug in to the system and control side. The process has four actuators and 10 sensors and the system reached rough equilibrium after a few seconds of simulation. The OMNeT++ network model was composed of a unit for each of these components talking wirelessly to a plant access point. These communicated with a central controller. The OMNeT++ bridges used real UNIX sockets to transfer data between the two simulations, with OMNeT++ keeping time. Below are the simulation results of the working model.

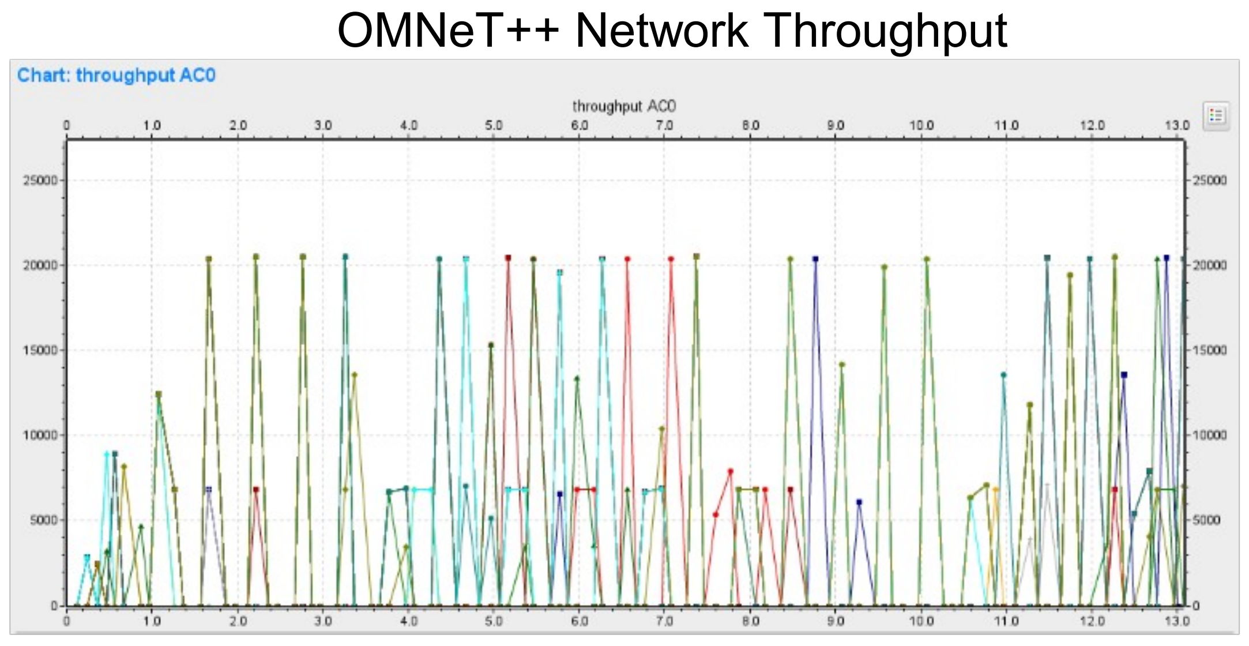
MATLAB Controller



MATLAB TE System



OMNeT++ Network Throughput



4. Results

Simulating the network with and without various attacks resulted in interesting results to the simulated Tennessee-Eastman process. During the DoS Attack, all packet traffic was lost and the process was not able to function. During the spoofing attack, a similar result of the process falling into chaos occurred. The graphs to the left illustrate these results.